

VICTOR JIH, State Bar No. 186515
Email: vjih@wsgr.com
SOPHIA M. MANCALL-BITEL, State Bar No. 337002
Email: smancallbitel@wsgr.com
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
1900 Avenue of The Stars, 28th Floor
Los Angeles, CA 90067
Telephone: (424) 446-6900
Facsimile: (866) 974-7329

ANTHONY J WEIBELL, State Bar No. 238850
Email: aweibell@wsgr.com
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
650 Page Mill Road
Palo Alto, California 94304-1050
Telephone: (650) 493-9300
Facsimile: (866) 974-7329

*Attorneys for Defendants
TikTok Inc. and ByteDance Inc.*

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, WESTERN DIVISION

BERNADINE GRIFFITH;
PATRICIA SHIH; RHONDA IRVIN;
MATHEW RAUCH; JACOB
WATTERS, individually and on
behalf of all others similarly situated,

Plaintiffs,

v.

TIKTOK, INC., et al.,

Defendants.

Case No.: 5:23-cv-00964-SB-E

**DEFENDANTS TIKTOK INC.
AND BYTEDANCE INC.'S
NOTICE OF MOTION AND
MOTION TO DISMISS
PLAINTIFFS' FIRST AMENDED
COMPLAINT UNDER FED. R.
CIV. P. 12(b)(6)**

Judge: Hon. Stanley Blumenfeld, Jr.
Date: December 15, 2023
Time: 8:30 a.m.
Place: Courtroom 6C

Action Filed: May 26, 2023
Trial Date: September 30, 2024

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on December 15, 2023 at 8:30 a.m., or as soon thereafter as the matter may be heard, before the Honorable Stanley Blumenfeld Jr. of the United States District Court for the Central District of California, Courtroom 6C, 350 West 1st Street, Los Angeles, California 90012, Defendants TikTok Inc. and ByteDance Inc. (together, “Defendants”) will move, and hereby do move, this Court pursuant to Federal Rule of Civil Procedure 12(b)(6) for an order dismissing the claims asserted by Plaintiffs Bernadine Griffith, Patricia Shih, Rhonda Irvin, Matthew Rauch, and Jacob Watters (together, “Plaintiffs”) in this action in their purported amended Class Action Complaint (ECF No. 63) (“FAC”) with prejudice for failure to state a claim.

Defendants’ Motion is based upon this Notice of Motion; the Memorandum of Points and Authorities in support thereof; the pleadings, records, and papers on file in this action; oral argument of counsel; and any other matters properly before the Court.

This Motion is made following the conference of counsel pursuant to Local Civil Rule 7-3 which took place on October 30, 2023, at which the parties were unable to resolve the substantive issues addressed in this Motion.

Respectfully submitted,

Dated: November 8, 2023

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: /s/ Victor Jih
Victor Jih

Attorney for Defendants
TIKTOK INC. and BYTEDANCE INC.

TABLE OF CONTENTS

		<u>Page</u>
1		
2		
3	I. INTRODUCTION.....	1
4	II. STATEMENT OF FACTS.....	3
5	A. TikTok and the TikTok Pixel.....	3
6	B. The Court’s Order on Defendants’ First Motion to Dismiss	3
7	C. Plaintiff’s First Amended Complaint.....	4
8	III. LEGAL STANDARD	5
9	IV. PLAINTIFFS FAIL TO STATE A CLAIM FOR COMMON LAW	
10	INTRUSION UPON SECLUSION OR A PRIVACY CLAIM UNDER	
	THE CALIFORNIA CONSTITUTION	7
11	A. Without A Misrepresentation, Plaintiffs Had No Reasonable	
12	Expectation of Privacy from Routine Record Data	7
13	B. Plaintiffs Fail to Allege That Any Sensitive Data Was Taken	9
14	C. Plaintiffs Cannot State a Privacy Violation Without Alleging	
	That Their Identifying Information Was Collected	11
15	V. PLAINTIFFS FAIL TO STATE INTERCEPTION CLAIMS	13
16	A. The CIPA Claims Fail Because Plaintiffs Do Not Allege That the	
17	“Contents” of Communications Were Intercepted or Recorded.....	13
18	B. Plaintiffs’ CIPA Claims Fail Because TikTok Did Not Use the	
	Pixel to Intercept or Record Any Communications.....	15
19	C. The Federal Wiretap Act Claim Fails for the Same Reasons	17
20	VI. PLAINTIFFS DO NOT STATE ANY PROPERTY CLAIM	17
21	VII. PLAINTIFFS DO NOT STATE A CFAA CLAIM.....	19
22	VIII. PLAINTIFFS DO NOT HAVE UCL STANDING	20
23	IX. PLAINTIFFS DO NOT STATE AN UNJUST ENRICHMENT	
24	CLAIM	21
25	X. CONCLUSION	22
26		
27		
28		

TABLE OF AUTHORITIES

Page(s)

CASES

<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	5
<i>Askins v. United States Dep't of Homeland Sec.</i> , 899 F.3d 1035 (9th Cir. 2018).....	6
<i>Astiana v. Hain Celestial Grp., Inc.</i> , 783 F.3d 753 (9th Cir. 2015).....	21, 22
<i>Brodsky v. Apple Inc.</i> , 445 F. Supp. 3d 110 (N.D. Cal. 2020)	17
<i>Calhoun v. Google</i> , 526 F. Supp. 3d 605 (N.D. Cal. 2021)	17
<i>City of L.A., Harbor Div. v. Santa Monica Baykeeper</i> , 254 F.3d 882 (9th Cir. 2001).....	6
<i>Cook v. GameStop, Inc.</i> , No. 2:22-cv-1292, 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023)....	10, 11, 14
<i>D'Angelo v. Penny Opco</i> , LLC, No. 23-cv-0981-BAS-DDL, 2023 WL 7006793 (S.D. Cal. Oct. 24, 2023)	10
<i>Dinerstein v. Google, LLC</i> , 73 F.4th 502 (7th Cir. 2023).....	12
<i>Doe I v. Sutter Health</i> , No. 34-2019-00258072-CU-BT-GDS, 2020 WL 1331948 (Cal. Super. Ct. Jan. 29, 2020)	8, 9, 11, 18
<i>Doe v. Meta Platforms, Inc.</i> , No. 22-cv-03580-WHO, 2023 WL 5837443 (N.D. Cal. Sept. 7, 2023) (Orrick, J.)	9
<i>E4 Strategic Sols., Inc. v. Pebble</i> , No. SA MC-15-00022-DOC, 2015 WL 12746706 (C.D. Cal. Oct. 23, 2015)	6
<i>Fraley v. Facebook, Inc.</i> , 830 F. Supp. 2d 785 (N.D. Cal. 2011)	18
<i>Gershzon v. Meta Platforms, Inc.</i> , No. 23-cv-00083-SI, 2023 WL 5420234 (N.D. Cal. Aug. 22, 2023)	14
<i>Gonzales v. Uber Techs., Inc.</i> , 305 F. Supp. 3d 1078 (N.D. Cal. 2018)	13

1	<i>Hammerling v. Google LLC</i> ,	
2	No. 21-cv-09004-CRB, 2022 WL 17365255 (N.D. Cal. Dec. 1, 2022), appeal filed, No. 22-17024 (9th Cir. Dec. 30, 2022)	9
3	<i>In re Facebook Inc. Internet Tracking Litig.</i> ,	
4	956 F.3d 589 (9th Cir. 2020).....	<i>passim</i>
5	<i>In re Hulu Privacy Litig.</i> ,	
6	86 F. Supp. 3d 1090 (N.D. Cal. 2015)	10
7	<i>In re iPhone Application Litig.</i> ,	
8	844 F. Supp. 2d 1040 (N.D. Cal. 2012)	13
9	<i>In re Meta Pixel Healthcare Litig.</i> ,	
10	647 F. Supp. 3d 778 (N.D. Cal. 2022)	14
11	<i>In re Meza</i> ,	
12	465 B.R. 152 (Bankr. D. Ariz. 2012)	18
13	<i>In re Zynga Privacy Litig.</i> ,	
14	750 F.3d 1098 (9th Cir. 2014).....	13
15	<i>Katz-Lacabe v. Oracle Am., Inc.</i> ,	
16	No. 22-cv-04792-RS, 2023 WL 2838118 (N.D. Cal. Apr. 6, 2023).....	10
17	<i>Knuttel v. Omaze, Inc.</i> ,	
18	No. 2:21-cv-09034-SB-PVC, 2022 WL 1843138 (C.D. Cal. Feb. 22, 2022)	21
19	<i>Kwikset Corp. v. Superior Ct.</i> ,	
20	51 Cal. 4th 310 (2011).....	20
21	<i>Liapes v. Facebook, Inc.</i> ,	
22	95 Cal. App. 5th 910 (2023).....	15
23	<i>Lightoller v. Jetblue Airways Corp.</i> ,	
24	No. 23-CV-00361-H-KSC, 2023 WL 3963823 (S.D. Cal. June 12, 2023)	12
25	<i>Lopez v. Apple</i> ,	
26	519 F. Supp. 3d 672 (N.D. Cal. 2021)	15
27	<i>Lopez v. Dang</i> ,	
28	No. SACV 21-353 JVS (KESx), 2022 WL 1567452 (C.D. Cal. Apr. 21, 2022)	5
	<i>Massie v. Gen. Motors LLC</i> ,	
	No. 21-787-RGA, 2022 WL 534468 (D. Del. Feb. 17, 2022)	9
	<i>Maui Jim, Inc. v. SmartBuy Guru Enters.</i> ,	
	No. 1:16 CV 9788, 2019 WL 5577165 (N.D. Ill. Oct. 29, 2019)	21
	<i>Miller v. Infinite Percent Partners, LLC</i> ,	
	No. 20-cv-02253-HSG, 2021 WL 2474440 (N.D. Cal. June 17, 2021)	5

1	<i>Oddei v. Optum, Inc.</i> ,	
2	No. 2:21-CV-03974-SB-MRW, 2021 WL 6103347	
	(C.D. Cal. Oct. 15, 2021) (Blumenfeld, J.)	6
3	<i>Popa v. PSP Grp., LLC</i> ,	
4	No. 23-cv-0294-JLR, 2023 WL 7001456	
	(W.D. Wash. Oct. 24, 2023).....	11, 12
5	<i>Sartori v. Schrodtt</i> ,	
6	424 F. Supp. 3d 1121 (N.D. Fla. 2019).....	19
7	<i>Schwartz v. Provident Life & Accident Ins. Co.</i> ,	
	216 Cal. App. 4th 607 (2013).....	20
8	<i>Sloan v. Gen. Motors LLC</i> ,	
9	No. 16-cv-07244-EMC, 2017 WL 3283998 (N.D. Cal. Aug. 1, 2017)	21
10	<i>Smith v. Facebook, Inc.</i> ,	
	262 F. Supp. 3d 943 (N.D. Cal. 2017)	8
11	<i>Sodexo Mgmt. v. Old Republic Ins. Co.</i> ,	
12	No. 20-cv-01517-WQH-BGS, 2022 WL 799425	
	(S.D. Cal. Mar. 15, 2022)	6
13	<i>Surf City Steel, Inc. v. Int’l Longshore & Warehouse Union</i> ,	
14	123 F. Supp. 3d 1219 (C.D. Cal. 2015), <i>aff’d</i> , 780 F. App’x 467	
	(9th Cir. 2019)	6
15	<i>TransUnion LLC v. Ramirez</i> ,	
16	141 S. Ct. 2190 (2021)	12
17	<i>U.S. v. Forrester</i> ,	
	512 F.3d 500 (9th Cir. 2008).....	8
18	<i>United States v. Abouammo</i> ,	
19	No. 19-cr-00621-EMC-1, 2022 WL 17584238	
	(N.D. Cal. Dec. 12, 2022).....	17, 18
20	<i>United States v. Green</i> ,	
21	12 F.4th 970 (9th Cir. 2021) (Paez, J., dissenting).....	17
22	<i>Vaquero Energy, Inc. v. Herda</i> ,	
	2015 WL 5173535 (E.D. Cal. Sept. 3, 2015).....	19, 20
23	<i>Varkonyi v. United Launch All., LLC</i> ,	
24	No. 23-cv-00359-SB-MRW, 2023 WL 4291649	
	(C.D. Cal. May 12, 2023) (Blumenfeld, J.).....	5
25	<i>Ventures Edge Legal PLLC v. GoDaddy.com LLC</i> ,	
26	No. CV-15-02291-PHX-GMS, 2017 WL 1075059	
	(D. Ariz. Mar. 22, 2017).....	6

STATUTES

18 U.S.C. § 1030(g)	19
Cal. Bus. & Prof. Code § 1798.120(a).....	18
Cal. Bus. & Prof. Code § 1798.140(v)(1).....	18
Cal. Penal Code § 631	13, 15
Cal. Penal Code § 632(a).....	13, 15

RULES

Fed. R. Civ. P. 12(b)(6)	5
Fed. R. Civ. P. 60.....	6
L.R. 7-18	6

MISCELLANEOUS

John Palfrey, <i>The Public and the Private at the United States Border with Cyberspace</i> , 78 Miss. L.J. 241, 260–61 (2008)	8
Richard T. Wang, <i>Cookies and Wires: Can Facebook Lure Users into Divulging Information Under the Wiretap Act’s Party Exception?</i> , 106 Cornell L. Rev. 1937, 1941-42 (2021).....	8
<i>Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies</i> , Art. II, Jan. 27, 1967, 18 U.S.T. 2410	18

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

The First Amended Complaint (“FAC”) makes clear that Plaintiffs’ claims against Defendants TikTok Inc. and ByteDance Inc. (together “Defendants” or “TikTok”) lack merit. The Court’s October 6 ruling on Defendants’ first motion to dismiss (“Order”) identified several areas that were either unclear or deficient. The Court allowed some of the claims to proceed and dismissed others with leave to amend. Plaintiffs’ new allegations bring clarity, but that clarity does not benefit Plaintiffs. If anything, Plaintiffs have pled themselves out of court.

The FAC now details how the Pixel functions when a website installs it without configuration. According to Plaintiffs, the Pixel automatically collects timestamp, user agent, referring and destination URLs, language, and Pixel session ID. This data sharing is not unique to the Pixel. It is the information passed alongside every online HTML request, to any website, whether it uses the TikTok Pixel or not. For the Internet to function, this information must be shared with a website and every computer and ISP along the way. Accessing any online information requires a location where the information can be found (URL), address indicating where the request should be returned (IP address), data about the device and the browser used to display the information (user agent / language), and some way to identify different sessions and associate them with a request (session ID).

Plaintiffs cannot state a privacy claim based solely on this type of data collection. This is routine information courts have held is not sensitive. This remains so even if an extensive amount of routine data is collected. With one exception, this is not information one can reasonably expect to be kept confidential, its collection offends no societal norm, and its disclosure reveals no content. The exception is the URL. Depending on how a website owner sets up the address for a webpage, its URL may or may not disclose sensitive or

1 substantive information. The FAC focuses on the collection of full-string URLs
2 that incorporate search terms as the way the Pixel could invade privacy rights, but
3 contains no allegations that any of the seven websites Plaintiffs visited actually
4 used full-string URLs or that those URLs included search terms. A claim cannot
5 be based on what could happen, but what actually did happen.

6 Yes, it is possible for a website owner to use the Pixel in a way that discloses
7 sensitive information about visitors to its web pages. But, as the FAC makes clear,
8 that only occurs if a website owner uses URLs that disclose such information or
9 specifically configures the Pixel to collect something beyond the routine data
10 identified above. The website owner makes those decisions. Any privacy
11 violation is caused by the website owner who chooses to use the Pixel in that
12 particular way, not TikTok who simply provides the tool.

13 For these reasons, none of Plaintiffs' privacy claims have merit and all
14 should be dismissed. That said, the claims fail for other reasons too. Plaintiffs
15 cannot claim larceny or conversion without property. A thing of value is not
16 "property" unless one has an exclusive right to it. The moon may be very valuable
17 for its resources, but it no more belongs to the United States than Russia or India.
18 Even assuming data has value, it is no more about Plaintiffs than the websites they
19 visit. Plaintiffs cannot state CFAA or UCL claims because they continue to rest on
20 speculative harms. The FAC can point to no real threat to public health or safety,
21 monetary loss to Plaintiffs, or concrete harm to their ability to participate in focus
22 groups or otherwise. Finally, there also is no independent unjust enrichment claim
23 because the FAC never alleges quasi-contract based on mistake, fraud, coercion or
24 request. It is entirely derivative and should be dismissed.

II. STATEMENT OF FACTS

A. TikTok and the TikTok Pixel

TikTok is an entertainment platform where users can create, view, and share videos. FAC ¶ 2. Companies advertise on the TikTok platform to reach TikTok users. *Id.* ¶ 23. To help them do so more effectively, TikTok offers websites a tool called the TikTok Pixel¹ to collect data about what those users do on their websites. *Id.* ¶ 46. The Pixel is a piece of code that website owners can choose to install onto their websites. *Id.* ¶¶ 46, 48-49. By configuring the Pixel, website owners also determine what data is shared with TikTok. *Id.* ¶¶ 52.

B. The Court's Order on Defendants' First Motion to Dismiss

Ms. Griffith filed her complaint on May 26, 2023, alleging that TikTok “secretly intercepted” or “stole” her “Private Data” through the Pixel. ECF No. 1 ¶¶ 75-76. She asserted seven claims: larceny, conversion, intrusion, constitutional invasion of privacy and violations of the California Invasion of Privacy Act (“CIPA”), federal Computer Fraud and Abuse Act (“CFAA”) and California Unfair Competition Law (“UCL”). *See id.* ¶¶ 99-152. On July 24, 2023, Defendants filed a motion to dismiss. ECF No. 24.

The Court issued its decision on October 6, 2023, granting in part and denying in part Defendants’ motion. Order at 19. Specifically:

- **Intrusion/Invasion of Privacy:** The Court allowed these claims to proceed on the theory that the Pixel can “amass a great degree of personalized information” including “an individual’s likes, dislikes, interests, and habits

¹ Plaintiffs broadly define the TikTok SDK to refer to use of the TikTok Pixel, Events API, and any other tool that may be used by websites to disclose information to TikTok. But Plaintiffs’ claims are based on the Pixel, not on any other tool. The FAC provides very little detail regarding the use of Events API or other tools, which is not surprising, since the Pixel is the only tool TikTok provides for use by websites. *Compare* FAC ¶¶ 45-54 *with* ¶ 58. TikTok therefore refers to the Pixel throughout. Nonetheless, these arguments apply equally to any claims Plaintiffs may have based on Events API or other tools. There are no allegations that any other tools exist or would give rise to materially different claims.

over a significant amount of time,” without giving a way to control
“unauthorized exploration of their private lives.” Order at 6-8.

- **CIPA:** The Court permitted Ms. Griffith’s Section 632 claim to proceed because it could not determine from the pleadings if “the websites’ decisions break the causal chain” from TikTok to the recording of a conversation. *Id.* at 11-12. The Court did not reach the Section 631 claim. *Id.* at 12.
- **Larceny/Conversion:** The Court upheld Ms. Griffith’s property claims based on a “growing trend across courts . . . to recognize the lost property value of personal information[]” and Ms. Griffith’s allegations that user data was valuable. *Id.* at 14-16.
- **CFAA:** Ms. Griffith’s CFAA claim was dismissed because she did not allege costs exceeding \$5,000 or any threat to public health or safety. *Id.* at 13-14.
- **UCL:** Ms. Griffith’s UCL claim was dismissed because she did not allege any actual financial loss. *Id.* at 17-19.

C. Plaintiff’s First Amended Complaint

On October 20, 2023, Plaintiffs filed the FAC, which adds four new Plaintiffs: Ms. Shih and Ms. Irvin, Mr. Rauch, and Mr. Watters. FAC ¶¶ 117, 126, 132, 140. These new Plaintiffs visited additional websites that installed TikTok’s Pixel. In addition to Hulu, Build-A-Bear, and Etsy, the FAC makes allegations about Rite Aid, Upwork, the Vitamin Shoppe, and Feeding America. FAC ¶¶ 110, 120, 128, 134-136, 142.

The FAC reasserts the same claims from the original complaint, including the previously dismissed CFAA and UCL claims. *Id.* ¶¶ 93-152. To save the CFAA claim, the FAC alleges a threat to public health and safety because one Plaintiff is a remote consultant for the Florida Department of Transportation (“DOT”) and has some internal network access. *Id.* ¶ 118. To save the UCL claim, the FAC alleges that three Plaintiffs lost the ability to participate in focus

1 groups or surveys. *Id.* ¶¶ 115, 124, 144. Plaintiffs also bring new claims under the
 2 Federal Wiretap Act and for unjust enrichment. *Id.* ¶¶ 220-35, 236-41.

3 The FAC provides greater detail on how the Pixel works. Specifically,
 4 Plaintiffs clarify exactly the information shared if a website installs the Pixel
 5 without further configuration: timestamp, user agent, URL, referrer URL,
 6 language, and a Pixel Session ID. *Id.* ¶ 49. The FAC confirms that to collect any
 7 information beyond this routine data, a website that installs the Pixel must
 8 specifically configure the Pixel. Websites can customize the Pixel to collect
 9 whatever they want, including 14 standard events. *Id.* ¶¶ 52, 230.

10 **III. LEGAL STANDARD**

11 The Court must dismiss a pleading that fails to state a claim upon which
 12 relief may be granted. *See* Fed. R. Civ. P. 12(b)(6). “[O]nly a complaint that
 13 states a plausible claim for relief survives a motion to dismiss.” *Ashcroft v. Iqbal*,
 14 556 U.S. 662, 679 (2009). Plaintiffs must allege sufficient and specific facts to
 15 allow this Court to evaluate the plausibility of her claims. *See Varkonyi v. United*
 16 *Launch All., LLC*, No. 23-cv-00359-SB-MRW, 2023 WL 4291649, at *2 (C.D.
 17 Cal. May 12, 2023) (Blumenfeld, J.). “There is no plausibility ‘where the well-
 18 pleaded facts do not permit the court to infer more than the mere possibility of
 19 misconduct.’” *Id.* (citing *Iqbal*, 556 U.S. at 679). While a court accepts as true all
 20 material allegations in the complaint, it need not accept the truth of conclusory
 21 allegations or unwarranted inferences. *Iqbal*, 556 U.S. 662 at 678-79. Moreover,
 22 “a plaintiff may plead himself out of court if he pleads facts which establish that he
 23 cannot prevail on his claim.” *Miller v. Infinite Percent Partners, LLC*, No. 20-cv-
 24 02253-HSG, 2021 WL 2474440, at *1 (N.D. Cal. June 17, 2021).

25 “Just as Plaintiffs may bring new allegations in its amended complaint, [a
 26 defendant] may present new arguments in his motion to dismiss, and the Court
 27 may rule on those arguments.” *Lopez v. Dang*, No. SACV 21-353 JVS (KESx),
 28

1 2022 WL 1567452, at *3 (C.D. Cal. Apr. 21, 2022). The new Plaintiffs’ claims—
 2 supported by facts specific to these individuals—have not been adjudicated before
 3 and concern different websites visited, activities performed, and information
 4 provided. Defendants are entitled to argue the legal validity of those claims
 5 because this Court is not bound to follow the holdings in its prior order. *Ventures*
 6 *Edge Legal PLLC v. GoDaddy.com LLC*, No. CV-15-02291-PHX-GMS, 2017 WL
 7 1075059, at *3 (D. Ariz. Mar. 22, 2017) (law of the case doctrine does not apply).

8 The court can and should also reconsider its prior rulings with respect to Ms.
 9 Griffith’s claims. *See City of L.A., Harbor Div. v. Santa Monica Baykeeper*, 254
 10 F.3d 882, 885 (9th Cir. 2001); Fed. R. Civ. P. 60; L.R. 7-18. In this District,
 11 reconsideration is appropriate if there are “new material facts or a change of law.”
 12 L.R. 7-18. Thus, it can be justified in light of the new allegations that apply to Ms.
 13 Griffith. *See Oddei v. Optum, Inc.*, No. 2:21-CV-03974-SB-MRW, 2021 WL
 14 6103347, at *3 (C.D. Cal. Oct. 15, 2021) (Blumenfeld, J.) (new fact allegations
 15 present “changed events and available defenses”); *Askins v. United States Dep’t of*
 16 *Homeland Sec.*, 899 F.3d 1035, 1043 (9th Cir. 2018) (“the district court [is] free to
 17 correct any errors or misunderstandings without having to find that its prior
 18 decision was ‘clearly erroneous.’”). It is also justified to the extent the Court’s
 19 fresh consideration of the new Plaintiffs’ claims yields a different result.

20 Reconsideration is warranted to avoid inconsistent rulings. *See, e.g., Sodexo*
 21 *Mgmt. v. Old Republic Ins. Co.*, No. 20-cv-01517-WQH-BGS, 2022 WL 799425,
 22 at *2 (S.D. Cal. Mar. 15, 2022) (staying case to avoid inconsistent rulings); *E4*
 23 *Strategic Sols., Inc. v. Pebble*, No. SA MC-15-00022-DOC (DFMx), 2015 WL
 24 12746706 (C.D. Cal. Oct. 23, 2015) (transferring case to avoid inconsistent
 25 rulings); *Surf City Steel, Inc. v. Int’l Longshore & Warehouse Union*, 123 F. Supp.
 26 3d 1219, 1236 n.12 (C.D. Cal. 2015) (reconsidering prior holding “[t]o the extent”
 27 inconsistent with ruling on new motion), *aff’d*, 780 F. App’x 467 (9th Cir. 2019).

1 **IV. PLAINTIFFS FAIL TO STATE A CLAIM FOR COMMON LAW**
 2 **INTRUSION UPON SECLUSION OR A PRIVACY CLAIM UNDER**
 3 **THE CALIFORNIA CONSTITUTION**

4 Ms. Griffith was allowed to proceed on her intrusion and privacy claims on
 5 the idea that the Pixel allowed TikTok “to amass a great degree of personalized
 6 information” including “an individual’s likes, dislikes, interests, and habits over a
 7 significant amount of time[.]” Order at 6. This Court denied TikTok’s motion
 8 because it was unclear if her allegations were “materially distinguishable” from
 9 those in *Facebook Tracking*. *Id.* at 7. But there are at least three material
 10 differences: unlike *Facebook Tracking*, Plaintiffs point to no misrepresentation that
 11 gave anyone a reason to expect privacy, no sensitive information that was actually
 12 collected, and no allegation that anything personally identifying was shared.

13 The FAC proceeds anyway, as if a large amount of routine data collected is
 14 enough to state a privacy claim. But these claims cannot be based on quantity
 15 alone. After all, collecting a lot of non-sensitive information that is not associated
 16 with any particular person does not, without some promise otherwise, violate any
 17 expectation of privacy or offend societal norms.

18 **A. Without A Misrepresentation, Plaintiffs Had No Reasonable**
 19 **Expectation of Privacy from Routine Record Data**

20 Plaintiffs’ claims turn on whether they plausibly allege a reasonable
 21 expectation of privacy. Order at 7. The inquiry depends on both the law and the
 22 facts, including the “circumstances of each case.” *In re Facebook Inc. Internet*
 23 *Tracking Litig.* (“*Facebook Tracking*”), 956 F.3d 589, 601 (9th Cir. 2020).

24 In *Facebook Tracking*, the Ninth Circuit found that Facebook’s false
 25 representations to its users created a reasonable expectation that Facebook would
 26 not “have access to the user’s individual data after the user logged out of the
 27 application.” 956 F.3d at 602; Order at 7. This Court recognized *Facebook*
 28 *Tracking*’s emphasis on Facebook’s privacy disclosures, which “failed to

1 acknowledge its tracking of logged-out users, suggesting that user’s information
 2 would not be tracked.” Order at 8. This Court held nonetheless that, even without
 3 a representation, certain tracking could still be “violative of social norms or
 4 expectations.” *Id.* Ms. Griffith’s claims proceeded despite her failure to allege
 5 reliance on any representations by TikTok.² The issue, then, was whether the data
 6 collected by the Pixel was so violative that she could state a claim for privacy
 7 without any representation or assurance.

8 The FAC confirms that the Pixel, without configurations, discloses only six
 9 pieces of data. FAC ¶ 49. Absent some specific representation, disclosing them
 10 violates no expectation of privacy or societal norm. Indeed, the sharing of this data
 11 is not unique to the Pixel or the websites that install it—it happens on every
 12 website and with every HTML request made to a browser to access information on
 13 the Internet. *See generally* Richard T. Wang, *Cookies and Wires: Can Facebook*
 14 *Lure Users into Divulging Information Under the Wiretap Act’s Party Exception?*,
 15 106 Cornell L. Rev. 1937, 1941-42 (2021). Because the Internet is a network of
 16 computers, this information necessarily passes through every routing computer
 17 along the way. *See* John Palfrey, *The Public and the Private at the United States*
 18 *Border with Cyberspace*, 78 Miss. L.J. 241, 260–61 (2008).

19 Courts, before and after *Facebook Tracking*, hold that such routine data
 20 cannot support a privacy claim. *See Doe I v. Sutter Health*, No. 34-2019-
 21 00258072-CU-BT-GDS, 2020 WL 1331948, at *9 (Cal. Super. Ct. Jan. 29, 2020)
 22 (describing online data sharing as “routine internet functionality”); *U.S. v.*
 23 *Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (no expectation of privacy in IP
 24 addresses of the websites visited); *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943,
 25 954 (N.D. Cal. 2017) (IP address, cookies, and browser fingerprinting);

26
 27 ² In fact, Plaintiffs are non-TikTok users. FAC ¶ 1. They have no knowledge of
 28 TikTok, the Pixel, or its use by any of the websites they visited. *See id.* ¶ 5. Thus,
 Plaintiffs cannot reasonably base any subjective expectation of privacy based on
 anything TikTok said or did.

1 *Hammerling v. Google LLC*, No. 21-cv-09004-CRB, 2022 WL 17365255, at *9
 2 (N.D. Cal. Dec. 1, 2022) (device type, carrier, and app installation).

3 **B. Plaintiffs Fail to Allege That Any Sensitive Data Was Taken**

4 To state a privacy claim, Plaintiffs must also “identify with specificity what,
 5 if any, private or particularly sensitive information about them [defendant]
 6 allegedly received.” *Doe v. Meta Platforms, Inc.*, No. 22-cv-03580-WHO, 2023
 7 WL 5837443, at *8 (N.D. Cal. Sept. 7, 2023). Conclusory allegations that “highly-
 8 confidential, sensitive, and personally identifiable communications” were collected
 9 are not enough. *Sutter Health*, 2020 WL 1331948, at *9. As this Court noted,
 10 *Facebook Tracking* rejected the argument “that the plaintiffs needed to identify
 11 specific sensitive information” collected. Order at 7. But that does not mean that
 12 sensitivity does not matter. Even if Plaintiffs cannot identify specific pieces of
 13 data, the Court can examine “whether the data itself is sensitive” and permit a
 14 privacy claim to proceed based on “the allegations that [the defendant] allegedly
 15 compiled highly personalized profiles from sensitive browsing histories and
 16 habits.” *Id.* (emphasis added).

17 *Facebook Tracking* confirms that Plaintiffs’ claims cannot be based on the
 18 collection of non-sensitive information. Plaintiffs can, of course, state a privacy
 19 claim by identifying specific sensitive information they shared and that was taken.
 20 *See* 956 F.3d at 603; *cf. Massie v. Gen. Motors LLC*, No. 21-787-RGA, 2022 WL
 21 534468, at *8-9 (D. Del. Feb. 17, 2022) (distinguishing *Facebook Tracking*
 22 because only browsing data collected, not personal information). Online
 23 consultations with a doctor can suffice. *See Meta Platforms, Inc.*, 2023 WL
 24 5837443, at *8. Alternatively, Plaintiffs may allege that the data collected could
 25 reveal sensitive information about them even without specifically identifying what
 26 data was taken. *Facebook Tracking* allowed this theory to proceed because of
 27 Meta Pixel’s ability to discern “sensitive and confidential” information from the
 28

1 seven million websites that employed the plug-in and the prevalence of full-string
 2 URLs including “the name of a website, folder and sub-folders on the web-server,
 3 and the name of the precise file requested.” 956 F.3d at 603.

4 The FAC fails to indicate the collection of sensitive information under either
 5 approach. As recently explained, even the collection of “sensitive, health-related”
 6 and “race and politics” information will not state a claim without allegations
 7 plaintiffs actually provided such information to websites which, in turn, was
 8 collected by a third party. *Katz-Lacabe*, 2023 WL 2838118, at *7. The FAC does
 9 not even identify any sensitive information that Plaintiffs entered on the websites
 10 they visited beyond conclusory allegations.

11 Nor does the FAC show that data collected can reveal sensitive information.
 12 It claims that the data collected, if it includes the full file path and search terms,
 13 could reveal “an incredible amount of private and personally identifiable
 14 information” like donations and food orders. FAC ¶ 50-51. But Plaintiffs never
 15 allege that the websites they visited in fact disclosed that data or otherwise
 16 disclosed sensitive information. And not a single Plaintiff has alleged that they
 17 made donations, ordered food on Grubhub, or entered particular search terms, and
 18 thus had any sensitive information that would be shared as a result.³ Allegations of
 19 information that could be taken have “little bearing” on the claims. Order at 8 n.4.

20 Without these specifics, the mere “collection and disclosure of a website
 21 visitor’s activity does not constitute the sort of highly objectionable conduct
 22 needed to state a claim” for intrusion. *Cook v. GameStop, Inc.*, No. 2:22-cv-1292,
 23 2023 WL 5529772, at *10 (W.D. Pa. Aug. 28, 2023); *D’Angelo v. Penny Opco*,

24
 25 ³ For example, Mr. Rauch viewed Feeding America videos. FAC ¶ 136. All the
 26 videos on Feeding America’s video gallery are embedded such that, no matter what
 27 video a user watches, the URL remains the same: <https://www.feedingamerica.org/about-us/press-room/our-videos>. Collecting URLs would not indicate what video
 28 was watched. The same goes for Ms. Griffith’s and Ms. Shih’s allegations that
 watching videos on Hulu somehow transmitted their private data because Hulu’s
 URLs are encrypted. FAC ¶¶ 111, 121; *In re Hulu Privacy Litig.*, 86 F. Supp. 3d
 1090, 1092-93 (N.D. Cal. 2015).

1 LLC, No. 23-cv-0981-BAS-DDL, 2023 WL 7006793, at *10 (S.D. Cal. Oct. 24,
 2 2023) (simply visiting a “public website owned and operated by a private
 3 company” is not the same as “private chats”). Searching and browsing on a public
 4 website like Rite-Aid or the Vitamin Shoppe is similar to searching on
 5 Webmd.com or Target.com. *See Sutter Health*, 2020 WL 1331948, at *9. There is
 6 no privacy claim that arises. *Cook*, 2023 WL 5529772, at *5.

7 **C. Plaintiffs Cannot State a Privacy Violation Without Alleging That**
 8 **Their Identifying Information Was Collected**

9 To state a privacy claim, Plaintiffs must allege that the information collected
 10 is personally identifying. This is necessary not only to state a claim, but to show a
 11 concrete injury for Article III standing. *See, e.g., Popa*, 2023 WL 7001456, at *5.

12 The Court has already recognized that the Pixel did not collect personal
 13 information like a phone number or email. Order at 8 n.4. And the FAC is devoid
 14 of allegations that Plaintiffs “enter[ed] any personally identifying information” on
 15 the websites they visited. *Cook*, 2023 WL 5529772, at *4. Nor do Plaintiffs allege
 16 that they provided any information that could somehow be identifiable. Not their
 17 “name,” “address,” “credit card information”—“nothing that could connect [their]
 18 browsing activity to [them].” *Cook* at *4. In effect, “everything [they] did on [the
 19 website] was completely anonymous.” *Id.*

20 Only two Plaintiffs allege that they made purchases (on Etsy and Vitamin
 21 Shoppe), FAC ¶¶ 112-113, 128, 135, but those barebones assertions provide no
 22 detail on what was required to make the purchase or even if they made those
 23 purchases in their own name, using their own credit card (as opposed to a spouse’s
 24 or family member’s). Browsing and searching online does not require the
 25 provision of personal information, nor are purchases necessarily reflected in
 26 browsing or search history. While some Plaintiffs allege that they are “member[s]”
 27 of or “paid subscriptions to” some websites they visited, see FAC ¶¶ 111-112, 120-
 28

1 121, 128, 142, none allege what a membership or a subscription entails, let alone
2 information it requires someone to provide to the website.

3 Plaintiffs' failure to plausibly allege that their personally identifying
4 information was provided to the websites ultimately raises questions of whether
5 Plaintiffs can even bring such claims. The Supreme Court recently clarified that a
6 bare violation of a statute cannot establish Article III standing. *TransUnion LLC v.*
7 *Ramirez*, 141 S. Ct. 2190, 2205 (2021). Courts have explained that, post-
8 *TransUnion*, *Facebook Tracking* is no longer good law in that there is no concrete,
9 particularized injury when data about online activity is collected unless the plaintiff
10 provided identifying information that can be combined with the online activity.
11 *See Popa*, 2023 WL 7001456, at *5; *see also Lightoller v. Jetblue Airways Corp.*,
12 No. 23-CV-00361-H-KSC, 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023) (no
13 standing based on collection of URLs, mouse movements, buttons clicked and text
14 entered on airline website which could not be tied to plaintiff); *Dinerstein v.*
15 *Google, LLC*, 73 F.4th 502, 513 (7th Cir. 2023) (expressing skepticism that the
16 collection of anonymized data could create any harm, let alone a concrete one).

17 This result makes sense, as the historically protected privacy right is the
18 right to control "information concerning [your] person." *Facebook Tracking*, 956
19 F.3d at 598. A plaintiff must "plead facts" demonstrating that the interception
20 amounts to an invasion of that right. *Popa*, 2023 WL 7001456, at *3. Without
21 that, it is information about an anonymous individual. *Facebook Tracking*, 956
22 F.3d at 598. Here, without any allegation that Plaintiffs provided Etsy, Rite Aid, or
23 any other website with specific information that personally identified them, none
24 has standing to pursue their intrusion claims. *See Popa*, 2023 WL 7001456, at *3.

V. PLAINTIFFS FAIL TO STATE INTERCEPTION CLAIMS

A. The CIPA Claims Fail Because Plaintiffs Do Not Allege That the “Contents” of Communications Were Intercepted or Recorded

CIPA prohibits the interception of the contents of a communication and the recording of the contents of a confidential communication. Cal. Penal Code §§ 631, 632(a). Gathering “information” is not enough. Plaintiffs must allege that the actual contents of communications are gathered. Thus, it is not enough to allege that a defendant collected information about products, videos, and opportunities Plaintiffs searched for, browsed for, purchased, or sold. *See* FAC ¶¶ 110-112, 120-122, 128; 134-136, 142. Plaintiffs must identify actual communications about those products, videos, and opportunities and allege that the contents of those communications were taken.

Courts draw a distinction between the contents of and record information about a communication. “Contents” refers to the actual substance of the communication. *See In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). “Record” information refers to its external, non-substantive characteristics, such as the parties involved, where it originated from, or its length. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012). For browsing activity, courts have held that the time a web page is accessed (timestamp), the device and browser used (user agent), the web page a visitor came from (referrer URL), the language used (user language), and the session (Pixel session ID) are all record information that do not reveal the contents of communications. *See In re Zynga Privacy Litig.*, 750 F.3d at 1105 (Facebook ID and referral URL not “contents”); *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1084-85 (N.D. Cal. 2018) (IP address and unique identifiers not “contents”).

Recognizing this, the FAC focuses on the Pixel’s collection of URL addresses. Whether a URL is “contents” or mere “record” information, however,

1 depends on how the owner of a website sets it up. The FAC alleges that full-string
 2 URL addresses can reveal the contents of communications, if the website owner
 3 sets up those addresses to include search terms used by a visitor. FAC, ¶¶ 47, 231.
 4 But more is required. It is “not enough” for Plaintiffs to “allege the potential
 5 capabilities” of a tool like the Pixel; rather, they must allege that the defendant “in
 6 fact, harnessed the capabilities [they] describe[], and it had the result of capturing
 7 the contents of specific communications.” *Cook*, 2023 WL 5529772, at *7 (W.D.
 8 Pa. Aug. 28, 2023) (emphasis added).

9 The FAC lacks specific allegations that the disclosure of URL addresses
 10 resulted in the disclosure of the contents of communications. There are no
 11 allegations that any of the seven websites visited actually used full-string URL
 12 addresses on the pages Plaintiffs visited; that those URLs were set up to include
 13 any search terms entered on those pages; that Plaintiffs even entered any search
 14 terms on these pages; that the website owners did not know how their URLs were
 15 set up when they installed the Pixel; that TikTok somehow controlled how those
 16 URLs would look; or that they were changed in any way because of the Pixel or
 17 TikTok. Without these allegations, the URLs at issue cannot be deemed
 18 “contents.” *Compare Gershzon v. Meta Platforms, Inc.*, No. 23-cv-00083-SI, 2023
 19 WL 5420234, at *3 (N.D. Cal. Aug. 22, 2023) (detailed examples of full-string
 20 URLs revealing contents) *with Cook*, 2023 WL 5529772, at *7 (allegations about
 21 “mouse movements, clicks, keystrokes [...], URLs” are insufficient because they
 22 lacked “critical necessary details”).

23 Plaintiffs’ failure to allege the “contents” of communications necessarily
 24 means they also fail to allege the contents of confidential communications, which
 25 is required under Section 632. The analysis of whether contents are confidential is
 26 similar to the analysis of a reasonable expectation of privacy. *See In re Meta Pixel*
 27 *Healthcare Litig.*, 647 F. Supp. 3d 778, 800 n.12 (N.D. Cal. 2022). Plaintiffs fail
 28

1 to plausibly allege that anything sensitive was shared, thus they also fail to allege
2 that the contents of anything confidential was recorded. *Supra* at Section IV.

3 **B. Plaintiffs' CIPA Claims Fail Because TikTok Did Not Use the**
4 **Pixel to Intercept or Record Any Communications**

5 To state CIPA claims against TikTok, Plaintiffs must allege that it was
6 TikTok who caused the interception, eavesdropping, or recording of the contents of
7 a communication. The salient language in Section 631 intentionally uses active
8 verbs and focuses liability on those “who willfully . . . reads, or attempts to read, or
9 to learn the contents or meaning of any message.” Cal. Penal Code § 631.

10 Similarly, Section 632 targets the person who “uses an electronic amplifying or
11 recording device to eavesdrop upon or record the confidential communication.” *Id.*
12 § 632(a). Indeed, the Legislature amended Section 632 in 2017 to change from the
13 passive and make it unambiguously active. *See* ECF No. 25, Ex. K (Assemb. Bill
14 No. 1671 (2015-2016 Reg. Sess.), as amended March 17, 2016).

15 The Court recognized this causation issue in its Order and asked for
16 additional authority and facts. Order at. 11 n.5. The causation issue does not arise
17 in most cases, which are brought against defendants who plainly engage in the acts
18 alleged to intercept or record. But where the defendant provides a tool used by
19 another, as here, causation must be more clearly articulated. In *Lopez*, Apple
20 “used” a recording device to eavesdrop or record a confidential communication by
21 “programming Siri software to intercept communications when no hot word was
22 spoken.” *Lopez v. Apple*, 519 F. Supp. 3d 672, 690 (N.D. Cal. 2021). Apple was
23 liable not for creating a tool, but for programming it to intercept communications
24 without being prompted, causing the recording of confidential communications.
25 Similarly, in *Liapes v. Facebook, Inc.*, Facebook was liable for intentional
26 discrimination because it pre-configured its ad targeting tool to work only if
27 advertisers first made discriminatory choices based on age, gender, and location.
28

1 95 Cal. App. 5th 910, 923 (2023). There, Facebook essentially forced advertisers
2 to use its tool in an unlawful way. *Id.*

3 In ruling on TikTok’s prior motion, this Court held that the pleading
4 contained insufficient facts to resolve “whether the websites’ decisions break the
5 causal chain from Defendants’ acts such that Defendants are insulated from
6 liability.” Order at 11-12. The FAC now gives details about how the Pixel works
7 with and without special configuration by websites. FAC ¶ 49. It acknowledges
8 that, of this list, only URLs have potential to disclose contents, which could occur
9 if the Pixel collects full-string URLs that may contain search terms used. *Id.* ¶¶ 47,
10 49. There is no allegation that the Pixel can be used to change the type of URL
11 used or that TikTok controls the type of URL a website uses.

12 In other words, the FAC confirms the Pixel is preset to limit the collection of
13 any information to the routine data that is always shared with any HTML request
14 on the Internet. To collect anything else, the website owner must make
15 configurations. FAC ¶ 45-49; ECF No. 25, Ex. A. These facts indicate that the
16 Pixel does not by default intercept or record the contents of any communications.
17 Whether it does so in a given instance depends on the specific URLs a website uses
18 or special action by a website. TikTok, however, is not the cause of any CIPA
19 violation. The website “break[s] the causal chain” for CIPA liability by choosing
20 to install the Pixel, deciding which pages to place it on, and configuring what it
21 wants the Pixel to collect in each instance. Order at 12.

22 That TikTok may recommend settings or encourage use of its Pixel does not
23 change this analysis. *See* Order at 11. There is no allegation that TikTok
24 encourages websites to use the Pixel in a way that violates CIPA. Instructions or
25 suggestions do not equate to the actual “use” of a device to eavesdrop, record, or
26 intercept. At best, they give rise to inducement, aiding and abetting, or other forms
27 of secondary liability. However, the FAC does not purport to state claims for
28

1 secondary liability under Section 631, nor does it allege facts that TikTok aided,
 2 agreed with, employed or conspired with the websites to intercept contents. As for
 3 Section 632, CIPA does not recognize secondary liability.

4 **C. The Federal Wiretap Act Claim Fails for the Same Reasons**

5 “The analysis for a violation of CIPA is the same as that under the federal
 6 Wiretap Act.” *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020).
 7 Thus, Plaintiffs’ Wiretap Act claim fails for the same reasons as the CIPA claims.
 8 *Supra* at Sections V.A, V.B. There is no need to analyze consent under the federal
 9 law, since Plaintiffs fail to allege that the contents of any communication
 10 (confidential or not) were intercepted, eavesdropped on, or recorded by TikTok.

11 **VI. PLAINTIFFS DO NOT STATE ANY PROPERTY CLAIM**

12 Plaintiffs cannot state larceny or conversion claims without the loss of
 13 property. Order at 14. The Court did not dismiss these claims given a “growing
 14 trend to recognize the lost property value of personal information.” *Id.* at 14-15
 15 (citing *Calhoun*, 526 F. Supp. 3d at 635). Yet, this trend has not changed the basic
 16 requirements for a property interest. The sine qua non for property remains a basis
 17 for “exclusive possession or control.” *United States v. Abouammo*, No. 19-cr-
 18 00621-EMC-1, 2022 WL 17584238, at *12 (N.D. Cal. Dec. 12, 2022).

19 Data about online browsing activity belongs no more to the person browsing
 20 than to the website browsed or the ISPs that uses it. While browsing data can be
 21 information about Plaintiffs, it is also information about the website visited, and
 22 because it is online, it is collected, logged, and shared by every device and ISP that
 23 comes in contact with it as it traverses to and from on the Internet. *See United*
 24 *States v. Green*, 12 F.4th 970, 977 (9th Cir. 2021) (Paez, J., dissenting) (the
 25 Internet involves a wide variety of communication and information retrieval
 26 methods). Plaintiffs cannot exclude those websites, devices, or ISPs from the data.

1 Without a claim to exclusivity, there is no basis for Plaintiffs to say
 2 anything—no matter how valuable—belongs to them. “The existence of value
 3 alone is not determinative” of a property right. *In re Meza*, 465 B.R. 152, 155-56
 4 (Bankr. D. Ariz. 2012). This is why no country can claim to own the Moon, even
 5 though its resources are extremely valuable. There is no basis to exclude others
 6 from possession. *See Treaty on Principles Governing the Activities of States in the*
 7 *Exploration and Use of Outer Space, Including the Moon and Other Celestial*
 8 *Bodies*, Art. II, Jan. 27, 1967, 18 U.S.T. 2410.

9 The cases identified in *Calhoun* as part of the “growing trend” reaffirm this
 10 exclusivity requirement. For example, in *Fraley*, the right of publicity conferred a
 11 right to exclude others from using the data at issue. *Fraley v. Facebook, Inc.*, 830
 12 F. Supp. 2d 785, 798-99 (N.D. Cal. 2011). Post-*Calhoun*, courts have similarly
 13 affirmed the exclusivity requirement. Thus, in *Abouammo*, a property right was
 14 based on a specific provision of the California Labor Code that recognized an
 15 exclusive interest in certain property acquired over the course of employment.
 16 *Abouammo*, 2022 WL 17584238 at *11.

17 The FAC alleges value but provides no basis for an “exclusive” right. FAC
 18 ¶ 88; *see Sutter Health*, 2020 WL 1331948, *14. The FAC tries to ground
 19 Plaintiffs’ property interests in the CCPA. But the CCPA does not help. It states
 20 that consumers can “direct a business that sells or shares personal information
 21 about the consumer to third parties not to sell or share the consumer’s personal
 22 information.” Section 1798.120(a); *see also* FAC ¶ 89. It limits the right of action
 23 to claims against businesses that sell or share personal information about a
 24 consumer to third parties. TikTok is not such a business and Plaintiffs do not
 25 allege as much. FAC ¶¶ 112, 120, 128, 134, 142. Moreover, the CCPA only
 26 applies to identifiable information. § 1798.140(v)(1). It cannot be used to control
 27 unidentifiable information that TikTok is not even able to associate with any
 28

1 person, let alone a non-TikTok user. Thus, Plaintiffs cannot assert a property right
2 that is greater than their ability to exclude others lawfully.

3 **VII. PLAINTIFFS DO NOT STATE A CFAA CLAIM**

4 The CFAA permits a private cause of action by a person who “suffers
5 damage or loss” because of unauthorized access to their computer if the losses
6 exceed \$5,000 or there is a threat to public health or safety. 18 U.S.C. § 1030(g);
7 Order at 12-13. The FAC abandons any attempt to allege losses over \$5,000.
8 Instead, Plaintiffs base the claim on the theory of a public threat alone. FAC ¶ 176.

9 This Court has addressed what is required to allege a plausible threat. It
10 gave examples of the types of allegations that might suffice: that a plaintiff “is a
11 federal employee or contractor, that the information gathered by TikTok may be
12 used to blackmail her or commit corporate espionage, or that it threatens to cause
13 physical or environmental harm.” Order at 14. Plaintiffs must allege that they
14 have access to important data, that a defendant’s unauthorized access implicates
15 that data, and the specific threat that arises because the defendant accesses that
16 data. *See* Order at 14; *Vaquero Energy, Inc. v. Herda*, 2015 WL 5173535, at *8
17 (E.D. Cal. Sept. 3, 2015); *Sartori v. Schrodts*, 424 F. Supp. 3d 1121, 1129 (N.D.
18 Fla. 2019) (dismissing CFAA claim because plaintiff failed to allege how
19 “accessing his Gmail account *per se* led to” loss or harm).

20 Only Ms. Shih attempts to allege a public threat, but she omits the specifics
21 the Court identified or any plausible theory of harm. Ms. Shih is a remote
22 consultant for the Florida DOT and has access to that agency’s network to use its
23 messaging and spatial planning software. FAC ¶ 118. As a result, her computer
24 has “some” access to the agency’s internal documents. *Id.* But there is no
25 allegation of access to any specific information accessed or explanation of how it
26 could be used to threaten public safety or health. She alleges that TikTok has
27 access to her browsing and search data from Etsy, Hulu, and Upwork—not data
28

1 from any government websites. *Id.* ¶ 120-122. She fails to explain how her visits
 2 to Hulu, Etsy, or Upwork could give TikTok access to restricted information
 3 unrelated to those commercial websites, that is not present on her computer, and
 4 can only be obtained through her limited access to networked computers. There is
 5 no allegation that she visited those websites while connected to DOT network.

6 This lack of specificity and plausible threat defeats the CFAA claim. This is
 7 nothing like *Vaquero*, where the defendant’s access to computer programs directly
 8 controlled “extensive and critical oil and gas production facilities” near homes and
 9 businesses. *Vaquero*, 2015 WL 5173535 at *8. Ms. Shih does not even identify
 10 the health or safety threat which could result from access to her data, let alone
 11 something like to “a H2S gas release, high pressure steam release, fire, oil spill, or
 12 pipeline rupture.” *Vaquero*, 2015 WL 5173535 at *8. Or, more accurately, she
 13 never identifies the threat that could result from access to her computer, which
 14 could have some access to unspecified data on her employer’s network.

15 **VIII. PLAINTIFFS DO NOT HAVE UCL STANDING**

16 This Court previously recognized that UCL standing is “substantially
 17 narrower” than Article III standing. Order at 16; *Kwikset Corp. v. Superior Ct.*, 51
 18 Cal. 4th 310, 324 (2011). The UCL requires the plaintiff to show they were
 19 “deprived of money or property to which [they had] a cognizable claim.” *Kwikset*,
 20 51 Cal. 4th at 323. This requires “actual financial losses.” Order at 18-19.
 21 “Purely speculative” injuries are insufficient. *Schwartz v. Provident Life &*
 22 *Accident Ins. Co.*, 216 Cal. App. 4th 607, 613 (2013).

23 Only three of the Plaintiffs try to claim actual financial losses based on
 24 allegations that their participation in focus groups and consumer surveys has been
 25 diminished because of the Pixel’s collection of their online browsing activity.
 26 FAC ¶¶ 115, 124, 144. But the FAC lacks specifics that would make this
 27 diminution plausible. There is no allegation that TikTok sells or shares any data or
 28

1 that it identifies who it collects from. There is no reason to believe anyone would
 2 be less likely to ask these Plaintiffs to participate in a focus group or survey as a
 3 result. There is no allegation that the browsing data and the focus groups and
 4 surveys these Plaintiffs are interested in even concern the same subjects. Ms.
 5 Griffith, for example, alleges that she participated in focus groups for “stoves and
 6 ovens, dog food, and curling irons.” FAC ¶ 115. But these products are unrelated
 7 to the websites she visited. Even if they were related, the FAC offers no reason to
 8 believe browsing data could take the place of a control-group inquiry. FAC ¶¶
 9 110-113. *See Maui Jim, Inc. v. SmartBuy Guru Enters.*, No. 1:16 CV 9788, 2019
 10 WL 5577165, at *2 (N.D. Ill. Oct. 29, 2019) (“A properly designed control group
 11 is . . . vital in a survey . . . about consumer behavior.”).

12 Without plausible allegations of financial loss, Plaintiffs cannot state valid
 13 claims under the UCL. These claims must therefore be dismissed.

14 **IX. PLAINTIFFS DO NOT STATE AN UNJUST ENRICHMENT CLAIM**

15 “California does not recognize a cause of action for unjust enrichment.”
 16 *Knuttel v. Omaze, Inc.*, No. 2:21-cv-09034-SB-PVC, 2022 WL 1843138, at *13
 17 (C.D. Cal. Feb. 22, 2022) (Blumenfeld J.). Thus, any separate unjust enrichment
 18 claim can be dismissed since it depends on the other claims. To the extent the
 19 unjust enrichment claim is derivative, it must fail for the same reasons the other
 20 claims fail. *Supra* at Section IV; *see Sloan v. Gen. Motors LLC*, No. 16-cv-07244-
 21 EMC, 2017 WL 3283998, at *10 (N.D. Cal. Aug. 1, 2017) (unjust enrichment
 22 claim dependent on a failed claim also fails).

23 While some courts claim to have recognized an independent claim for unjust
 24 enrichment, they have done so only when such claims are limited to “a quasi-
 25 contract claim seeking restitution.” *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d
 26 753, 762 (9th Cir. 2015) (citation omitted). However, Plaintiffs make no reference
 27 to “quasi-contract” claims in the FAC. Nor is there any allegation that Defendants
 28

1 have “been unjustly conferred a benefit through mistake, fraud, coercion, or
2 request.” *Astiana*, 783 F.3d at 762. Thus, this claim fails.

3 **X. CONCLUSION**

4 For all these reasons, the FAC must be dismissed.

5
6 Dated: November 8, 2023

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

8 By: /s/ Victor Jih

9 Victor Jih

10 *Attorney for Defendants*

11 TIKTOK INC. and BYTEDANCE INC.
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATION OF MEET AND CONFER

I certify that the parties met by videoconference on October 30, 2023, thoroughly discussed each and every issue raised in the motion, and attempted in good faith to resolve the motion in whole or in part.

Dated: November 8, 2023

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: /s/ Victor Jih

Victor Jih

Attorney for Defendants

TIKTOK INC. and BYTEDANCE INC.

CERTIFICATE OF COMPLIANCE

The undersigned, counsel of record for Defendants TikTok Inc. and ByteDance Inc., certifies that this brief contains 7,000 words, which complies with the word limit of L.R. 11-6.1.

Dated: November 8, 2023

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: /s/ Victor Jih

Victor Jih

Attorney for Defendants

TIKTOK INC. and BYTEDANCE INC.